Check Point® VPN-1 SecureClient for Mac OS X
Release Notes

November 1, 2004

This document contains important information not included in the documentation. Review this information before setting up SecureClient for Mac OS X.

IMPORTANT
Check Point recommends that customers stay up-to-date with the latest service packs, hotfixes and versions of security products, as they contain security enhancements and protection against new and changing attacks.

In This Document

IMPORTANT
Before you begin, read the latest available version of these release notes at:
http://www.checkpoint.com/techsupport/downloads.jsp

Introduction

This version of SecureClient for Mac OS-X (Panther) is based on SecureClient R56 and derive most of its connectivity and security functions.

The version has a new GUI based on a cross-platform GUI framework.

Authentication is supported in the following modes: pre-shared secret, hybrid mode, certificates, SecureID and Challenge-Response.

MEP, UDP encapsulation, TCPT and other connectivity options are supported.

In case the Gateway requires its clients to have a Secured Configuration (SCV), the client will be allowed to open connections only if the configuration on the management allows it explicitly. See “Frequently Asked Questions” on page 6 for more details.

The client supports connections over various network cards such as Ethernet, Dialup and AirPort.

SecureClient for Macintosh OS X requires a separate license (SKU - CPVP-VMC-xx-xx). Please be sure to install the proper license on the management module in order to comply with the End User License Agreement and prevent malfunctions.

System Requirements

OS: Mac OS-X 10.3.x (Panther)

Minimum disk space: 100 MB

Minimum memory requirements: 128 MB

Installation Guide

The installation package `SecureClient_R56.B*.pkg.zip` is a self extracting package containing the SecureClient installer.

Installing SecureClient:

1. Copy the zip file to the desktop, or any other directory accessible from Finder. Double-click on the zip file, the package would unzip and the installer application would run.
2. Follow the instructions on the screen, enter an admin user user-name and password, when required.
3. The final part of the wizard might take a few minutes to complete.
4. Reboot the machine.

Uninstalling SecureClient:

Double-click on the uninstaller icon in the Check Point folder in Applications. The Installer runs in a Terminal Application window. In case the user running the uninstaller is non-admin the installer would request an admin user name and password before uninstaller can continue. After uninstaller is finished, reboot the machine.

Using SecureClient

SecureClient for Mac OS-X uses three processes to work: Two daemons called 'SR_Service' and 'SR_Watchdog', started at boot time using root credentials, and a GUI application SecureClient runs by the user in a logon-session. Using the GUI the user is allowed to do various operations "on" the daemon, depending on the permissions set by the system administrator.

The SecureClient GUI is an application that can be run by clicking the SecureClient icon from the Applications folder in Finder. The GUI is automatically run when a user logs into the machine.

When the GUI is running a menu-icon is placed on the menu. Most of SecureClient's functions can be accessed from the menu that appears when clicking the icon.

For detailed description of SecureClient functions and dialogs, please refer to the User Manual accessible by any of the **HELP** buttons on the different menus, and from the Menu-icon Help menu.

Desktop Security Policy: When connecting to a site, a logon to its policy server is also attempted, and a desktop policy is downloaded if possible. The policy is then enforced whether the user is connected or disconnected. Such a policy may restrict the user's ability to connect to various network resources.

Known Limitations

The following features are not supported in SecureClient for Mac OS-X:

- SecuRemote variation (SecureClient can connect to all SecuRemote configurations)
- Compact View (Extended View only)
- Software updates (SDS)
- Auto Local Logon (SSO)
- Secure Domain Logon (SDL)
- Entrust, SoftID and SAA (OPSEC) authentication schemes
- Hardware Token authentication
- The client does not run Secure Configuration (SCV) tests
- Installation options (`product.ini`)
- Packet drop indication in the taskbar icon
- Profile export / import / desktop shortcut
- Partial topology
- Hotspots registration
- Dialup integration
- User is unable to connect to site when using IP over FireWire as the main interface

- IPv6 is not filtered by SecureClient firewall (rules are not enforced).

Known Issues

- Connection with Office Mode over FireWire IP connection is not supported. The connection fails.
- When working with a Visitor Mode profile and Manual Proxy settings in a MEP configuration: If the primary GW is down, connections into the encryption domain are dropped.
- Only one dialog can be opened from SecureClient menu icon at any time. If a dialog is already open clicking on any command would bring up the open dialog to the foreground.
- SecureClient GUI crashes when using it with some Application Enhancer (by UNSANITY) Plug-in. If you are using this software, add SecureClient to the Exclude List of the plug-in.
- Machine will not go to sleep (stand-by) on inactivity when turning on SecureClient logging (in **Setting > Advanced**) and when desktop policy includes rules with LOG directive that are frequently matched. This happens since these activities require writing data to the hard drive, and so it does not go into idle state.
- SecureClient GUI writes some data into the user's `Console.log`. This has no apparent effect on the application and the user experience.
- When connecting with a 'Route all traffic through gateway' profile to a domain with MEP configuration, if the gateway the client is connecting to is down, or the gateway the client is connected to "falls", the user may not be correctly notified and automatic switching of gateways may not happen.

CLI Environment

Most of the GUI commands can also be done using a command-line based utility `scc`.

In order to execute the `scc` command, one should define the following environment variables (for example, initialize in your tcshell login `.cshrc` file with the following commands):

```
setenv CPDIR /opt/CPsrsc-50
setenv FWDIR $CPDIR
setenv SRDIR $CPDIR
setenv FW_BOOT_DIR $CPDIR/boot
setenv CPMDIR $CPDIR
setenv TMPDIR /tmp
setenv PATH $FWDIR/bin:$FWDIR/lib:$PATH
setenv DYLD_LIBRARY_PATH $CPDIR/bin
setenv CPTMPDIR $SRDIR/tmp
```

The script can be found in the client install directory and loaded using the command:

```
source /opt/CPsrsc-50/.cshrc
```

To check SecureClient daemon status, run the command:

```
scc status
```

a "normal" output would be:

VPN-1 is disconnected

If the status reads **SecureClient services are down** you can use the `scc startsc` command to start the daemon.

For the full list of CLI usage, type scc at command prompt without any parameters.

Troubleshooting

Auditing Sessions

There are several options to view the status of SecureClient

TABLE 1 SecureClient Status Commands

Command	Meaning
`scc status`	gives brief status
`scc setpolicy`	displays whether desktop policy is currently enabled
`scc setmode`	displays current mode

- To enable logging of SecureClient processes use the Advanced tab in the Client Settings dialog. You can also manually create an empty file with the name `sr_tde.all` in the `$SRDIR` and restart the daemon/GUI. Logs are collected in the `$SRDIR/log` folder and can also be viewed from `/var/log/SecureClient` using the Console application.

- The script `/opt/CPsrsc-50/bin/envelope` can be used instead of the "rotating key" of the windows version. It's output reads:

[VPN] Envelope: Idle

[VPN] Envelope: Encrypting

- The file `/opt/CPsrsc-50/log/sr_service_tde.log` (located in `/opt/CPsrsc-50/log`) collects debugging information during the operation of SecureClient.

- The file `/opt/CPsrsc-50/log/ScBootlog.txt` (located in `/opt/CPsrsc-50/log`) contains more debugging information, to complement the information in `sr_service_tde.log`.

- To collect IKE logs create an empty file with the name `fwike_debug.all` in the `$SRDIR` and restart the daemon. The log file is called `ike.elg`.

The command srfw can be used in many ways. A few of the common useful commands are:

TABLE 2 fw Commands

Command	Meaning
`srfw monitor`	collect FW logs
`srfw monitor -p all`	on all “chain” stages
`srfw monitor -o /tmp/log.eth`	output as Ethereal log file
`srfw stat`	show enforced FW policy
`srfw ctl iflist`	list attached interfaces
`srfw ctl install`	attach to all interfaces
`srfw ctl uninstall`	detach from all interfaces

Note - `srfw` commands run only in root user, after setting the above environment variables.

- The script **kernel** can be used to simplify collection of fw kernel logs. Run it using the command: `sh /opt/CPsrcr-50/bin/kernel`

- The script **monitor** can be used to simplify collection fw traffic as Ethereal log. Run it using the command: `sh /opt/CPsrcr-50/bin/monitor`

Mac OS-X operations:

- To change your users' shell to `tcsh` use the `chsh` command, and edit the Shell entry to `/bin/tcsh`.
- To make the CP environment script run when the user starts a terminal session, use the command `ln -s /opt/CPsrsc-50/.cshrc ~/.cshrc`.
- To enable the root user, use the utility program NetInfo Manager, select **Security->Enable Root User**.
- To allow a user to 'sudo' use NetInfo Manager (found under Applications/Utilities): under **groups > admin** add the user name to the **users** list

Frequently Asked Questions

Q1: My Gateway supports VPN connections with SecuRemote. Will you be distributing SecuRemote with this build of SecureClient?

A1: SecureClient can connect to any Gateway that supports SecuRemote connections. A SecuRemote version of SecureClient for Macosx is not planned.

Q2: I have a customized userc.C on clients running SecureClient for Windows.

Can I use the same database file on my SecureClient for Macosx?

A2: Yes. SecureClient for Macosx supports the same userc.C format as SecureClient for Windows R56. Note that some of the windows' features are not supported on the Macosx release. When you do this procedure please note the following issues: (1) The format of a

text file on UNIX machines is different than the format used on Windows machines, so you have to dos2unix the userc.C file before you use it in the mac client, and that (2) the mac client works in what is called CLI Mode. We even added a script that can help in the process. Please follow this procedure when transferring a userc.C file from Windows to Macosx:

1. On the win machine switch to CLI mode:
   [c:\program files\checkpoint\securemote\bin]scc setmode cli
2. Copy the file from the win machine to the mac machine into (/tmp in this example)
3. On the Macosx open terminal and run the following commands as root:
   `# tcsh` - run in tcsh
   `# source /opt/CPsrsc-50/.cshrc` - add environment vars
   `# scc stop` - stop secure client
   `# cp $SRDIR/database/userc.C $SRDIR/database/userc.C.bak` - backup current userc.C
   `# mv /tmp/userc.C $SRDIR/database` - replace userc.C
   `# $SRDIR/bin/cpdos2unix $SRDIR/database/userc.C` - dos2unix the file
   `# scc start` - start secure client
4. In Finder, run SecureClient GUI from Applications.

Q3: How do I change the boot policy to a restrictive policy?

A3: The default boot policy, when installing SecureClient for Macosx is "accept all" (same as Windows client). Macosx comes packaged with two policy files in the `$SRDIR/conf folder`: `sc_boot_acceptall.bin` ("accept all") and `sc_boot_blockinbound.bin` (block inbound connections). The link `$SRDIR/default.bin` points to one of them and is used as the effective boot policy file. To change the boot policy one can change the link to point to `sc_boot_blockinbound.bin` after the client is already installed.

Q4: How do I stop SecureClient form Automatically starting up when I log in?

A4: Starting up the SecureClient GUI is done by adding the GUI application to the list of applications run by any user on log-in. If you'd like to change this behavior you may do the following, Start a terminal application and change to root; then:

```
# tcsh
# source /opt/CPsrsc-50/.cshrc
# StartupItemsMgr remove $SRDIR/bin/SecureClient.app
```

Now, if you would like to add automatic GUI startup to just one user, you can add it to the user's startup items, from system-preferences -> Users applet.

Note that this procedure will only effect the launching of the SecureClient GUI. The daemons will still be running as usual.

Q5: How can I enforce desktop rules on my IPv6 network interfaces?

A5: SecureClient for Macosx does not enforce rules on IPv6 traffic.

Q6: After installing SecureClient for Macosx my machine gets stuck with a grey screen, requesting that I reboot the machine. This is happening on every reboot, so I cannot uninstall SecureClient from the Finder. How do I uninstall SecureClient without reinstalling the whole machine?

A6: There is no need to reinstall the machine. Follow this procedure:

1. Turn the machine off and back on.
2. You are now in Single User Mode. Hold down the "Apple" key along with "S" key for a few seconds, until you see a black screen containing a few lines of text.
3. type:

   `# /bin/fsck -yf` - may take several minutes

   `# /sbin/mount -uw /`

   `# mv /opt /opt2` - renames the SecureClient installation folder

   `# reboot` - reboot machine

Now the machine should be able to boot, as SecureClient is no longer loaded.

You still need to uninstall:

4. Open a terminal window and type:

   `# sudo mv /opt2 /opt` - enter your password when prompt; restores folder

5. Now uninstall SecureClient. Using the Finder, open the "Applications" folder, then "Check Point SecureClient" folder, then click "Uninstall SecureClient".

Q7: My gateway blocks traffic from clients that do not pass Secure Configuration (SCV) tests. How do I configure the Gateway to allow such traffic from my Mac OS clients?

A7: On the Gateway's management, open the `local.scv` file (located in `$FWDIR/conf`). In the "SCVGlobalParams" section, add the following field - ":allow_non_scv_clients (true)". When you're done editing, save the file, and install the Desktop Security Policy on the relevant gateway (using Checkpoint's SmartDashboard). Once the policy is installed, traffic from Mac OS clients will be allowed even if SCV is enforced.

Q8: How can I use Entrust Digital ID with this client release?

A8: Customers using Entrust Digital ID's in the *.epf format need to export them into *.p12 format using the Entrust Entelligence 6.0 'Export' feature. The Export feature is accessed by right clicking on the Entrust key Tray icon and selecting Entrust Options. Users

must have their account configured with suitable export policies by their PKI administrator before the PKCS#12 Export feature is enabled in Entrust Entelligence. Please refer to the Entrust document "Desktop Admin Guide 6.0" for configuration instructions for Entrust/Authority 5.0 and 6.0. Relevant sections are titled "Export to PKCS#12" and "Enabling the Export Certificate Type".

Q9: How can I use *Rendezvous* after applying a block inbound desktop security policy?

Q9: Block inbound desktop security policy doesn't allow incoming connections to your desktop machine. *Rendezvous* requires IP multicast traffic to function properly. To support *Rendezvous*, add a desktop security rule above the block inbound rule:

Source: (IP: 224.0.0.0-224.0.0.255, 239.0.0.0-239.255.255.255)

Dest: All_Users@Any

Service: Tcp, Udp

Action: Accept

This will allow the necessary incoming multicast connections for *Rendezvous*.

Q10: How can I configure SecureClient to not appear in the Doc?

A10: You may follow the procedure below to make SecureClient GUI not appear in the Doc. Note that this would limit your ability to get into open dialogs by using the Apple+Tab and click on SecureClient menu icon when it is hidden by other applications' menus.

1. Open Terminal Application and execute the command:

```
# open /opt/CPsrsc-50/bin/SecureClient.app/Contents
```

2. Double-click the `Info.plist` file to open it (opened in Property List Editor). Add a new sibling to root with the following parameters:

   Key: LSUIElement

   Class: String

   Value: 1

3. Save the `Info.plist` file using **File > Save** and quit the application.

4. Again, in Terminal Application execute the command:

```
# touch /opt/CPsrsc-50/bin/SecureClient.app
```

5. If SecureClient GUI is running menu-click its icon in the Doc and choose **Quit**.

6. Run SecureClient GUI from the Applications menu in Finder.